OIPE JC168
APR 17 2001
PATENT & TRADEMARK OFFICE

CFO1500 2US
RECEIVED
APR 19 2001
Technology Center 2600

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９９年１２月２７日

出願番号
Application Number: 平成１１年特許願第３７１７８０号

願人
Applicant (s): キヤノン株式会社

CERTIFIED COPY OF PRIORITY DOCUMENT

２００１年　１月１９日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２０００－３１１４２９０

【書類名】　特許願
【整理番号】　4120042
【提出日】　平成11年12月27日
【あて先】　特許庁長官殿
【国際特許分類】　H04N　5/00
【発明の名称】　画像処理システム、画像処理方法、メモリカード及び記憶媒体
【請求項の数】　22
【発明者】
【住所又は居所】　東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内
【氏名】　笠井　一宏
【特許出願人】
【識別番号】　000001007
【氏名又は名称】　キヤノン株式会社
【代理人】
【識別番号】　100090273
【弁理士】
【氏名又は名称】　國分　孝悦
【電話番号】　03-3590-8901
【手数料の表示】
【予納台帳番号】　035493
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9705348
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　画像処理システム、画像処理方法、メモリカード及び記憶媒体

【特許請求の範囲】

【請求項１】　メモリ媒体にアクセス可能なインターフェースを備えた画像処理システムであって、

上記メモリ媒体に蓄積されている画像ファイルデータに関する電子署名、上記電子署名に用いた秘密鍵、または上記秘密鍵と対となる公開鍵を、上記画像ファイルデータ及びプロパティファイルとともに読み出す情報読み出し手段と、

上記情報読み出し手段によって読み出された情報に基づいて画像の出力を行う画像出力制御手段とを具備することを特徴とする画像処理システム。

【請求項２】　上記情報読み出し手段によって読み出された上記画像ファイルデータに関する電子署名を、上記公開鍵を用いて復号化する電子署名復号化手段を具備することを特徴とする請求項１に記載の画像処理システム。

【請求項３】　上記画像ファイルデータから得られる画像ファイル固有のメッセージダイジェスト値を、一方向性関数を用いて算出するメッセージダイジェスト値算出手段を具備することを特徴とする請求項１または２に記載の画像処理システム。

【請求項４】　上記画像ファイルデータの電子署名を復号化する電子署名復号化手段と、

上記電子署名復号化手段によって得られるデータ値と上記メッセージダイジェスト値とを比較する比較手段と、

上記比較手段の比較結果に基づいて、上記画像ファイルデータの検証を行う画像ファイルデータ検証手段とを具備することを特徴とする請求項３に記載の画像処理システム。

【請求項５】　メモリ媒体にアクセス可能なインターフェースを備えた画像処理システムであって、

上記インターフェースに対する上記メモリ媒体の接続を検出するメモリ媒体検出手段と、

上記メモリ媒体検出手段により上記メモリ媒体の接続が検出された場合に、上

記メモリ媒体に蓄積されている画像ファイルデータに関する電子署名、上記電子署名に用いた秘密鍵、またはその対となる公開鍵を、上記画像ファイルデータ及びプロパティファイルとともに転送する情報読み出し手段と、

上記情報読み出し手段よって読み出された情報に基づいて画像出力を行うように制御する画像出力制御手段とを具備することを特徴とする画像処理システム。

【請求項６】　メモリ媒体にアクセス可能なインターフェースを備えた画像処理システムであって、

上記メモリ媒体に保存する画像ファイルデータを作成する画像ファイルデータ作成手段と、

上記画像ファイルデータ作成手段によって作成された画像ファイルデータを記憶手段に保存する画像ファイルデータ保存手段と、

上記画像ファイルデータから得られる画像ファイル固有のメッセージダイジェスト値を、一方向性関数を用いて算出するメッセージダイジェスト値算出手段と、

上記メッセージダイジェスト値算出手段により算出されたメッセージダイジェスト値を、上記記憶手段内に格納された秘密鍵で暗号化するデジタル署名生成手段とを具備することを特徴とする画像処理システム。

【請求項７】　上記デジタル署名生成手段によって作成されたデジタル署名をプロパティファイルに格納するデジタル署名格納手段と、

上記デジタル署名が格納されたプロパティファイルを上記メモリ媒体内のプロパティ領域に保存する第１の保存手段と、

上記メモリ媒体内の画像ファイル領域に署名対象画像ファイルデータを保存する第２の保存手段とを具備することを特徴とする請求項６に記載の画像処理システム。

【請求項８】　上記メッセージダイジェスト値を暗号化するための秘密鍵は機器固有の秘密鍵であることを特徴とする請求項１～７の何れか１項に記載の画像処理システム。

【請求項９】　上記メッセージダイジェスト値を暗号化するための秘密鍵をユーザ定義により新規に作成する秘密鍵作成手段を具備することを特徴とする請

求項１～７の何れか１項に記載の画像処理システム。

【請求項１０】　メモリ媒体にアクセス可能なインターフェースを備えた画像処理システムにおける画像処理方法であって、

上記メモリ媒体に蓄積されている画像ファイルデータに関する電子署名、上記電子署名に用いた秘密鍵、または上記秘密鍵と対となる公開鍵を、上記画像ファイルデータ及びプロパティファイルとともに読み出す情報読み出し処理と、

上記情報読み出し処理によって読み出された情報に基づいて画像の出力を行う画像出力制御処理とを行うことを特徴とする画像処理方法。

【請求項１１】　上記情報読み出し処理によって読み出された上記画像ファイルデータに関する電子署名を、記憶手段に格納された公開鍵を用いて復号化する電子署名復号化処理を行うことを特徴とする請求項１０に記載の画像処理方法。

【請求項１２】　上記画像ファイルデータから得られる画像ファイル固有のメッセージダイジェスト値を、一方向性関数を用いて算出するメッセージダイジェスト値算出処理を行うことを特徴とする請求項１０または１１に記載の画像処理方法。

【請求項１３】　上記画像ファイルデータの電子署名を復号化する電子署名復号化処理と、

上記電子署名復号化処理によって得られるデータ値と上記メッセージダイジェスト値とを比較する比較処理と、

上記比較処理の比較結果に基づいて、上記画像ファイルデータの検証を行う画像ファイルデータ検証処理とを行うことを特徴とする請求項１２に記載の画像処理方法。

【請求項１４】　メモリ媒体にアクセス可能なインターフェースを備えた画像処理システムにおける画像処理方法であって、

上記インターフェースに対する上記メモリ媒体の接続を検出するメモリ媒体検出処理と、

上記メモリ媒体検出処理により上記メモリ媒体の接続が検出された場合に、上記メモリ媒体に蓄積されている画像ファイルデータに関する電子署名、上記電子

署名に用いた秘密鍵、またはその対となる公開鍵を、上記画像ファイルデータ及びプロパティファイルとともに転送する情報読み出し処理と、

上記情報読み出し処理よって読み出された情報に基づいて画像出力を行うように制御する画像出力制御処理とを行うことを特徴とする画像処理方法。

【請求項１５】　メモリ媒体にアクセス可能なインターフェースを備えた画像処理システムにおける画像処理方法であって、

上記メモリ媒体に保存する画像ファイルデータを作成する画像ファイルデータ作成処理と、

上記画像ファイルデータ作成処理によって作成された画像ファイルデータを記憶手段に保存する画像ファイルデータ保存処理と、

上記画像ファイルデータから得られる画像ファイル固有のメッセージダイジェスト値を、一方向性関数を用いて算出するメッセージダイジェスト値算出処理と、

上記メッセージダイジェスト値算出処理により算出されたメッセージダイジェスト値を、上記記憶手段内に格納された秘密鍵で暗号化するデジタル署名生成処理とを行うことを特徴とする画像処理方法。

【請求項１６】　上記デジタル署名生成処理によって作成されたデジタル署名をプロパティファイルに格納するデジタル署名格納処理と、

上記デジタル署名が格納されたプロパティファイルを上記メモリ媒体内のプロパティ領域に保存する第１の保存処理と、

上記メモリ媒体内の画像ファイル領域に署名対象画像ファイルデータを保存する第２の保存処理とを行うことを特徴とする請求項１５に記載の画像処理方法。

【請求項１７】　上記メッセージダイジェスト値を暗号化するための秘密鍵は機器固有の秘密鍵であることを特徴とする請求項１０～１６の何れか１項に記載の画像処理方法。

【請求項１８】　上記メッセージダイジェスト値を暗号化するための秘密鍵をユーザ定義により新規に作成する秘密鍵作成処理を行うことを特徴とする請求項１０～１６の何れか１項に記載の画像処理方法。

【請求項１９】　電子署名が施された画像ファイルデータが格納されている

ことを特徴とするメモリカード。

【請求項２０】　画像ファイルデータと、上記画像ファイルデータに関する電子署名と、上記電子署名に用いた秘密鍵と、上記秘密鍵と対となる公開鍵と、上記画像ファイルに係わるプロパティファイルとが格納されていることを特徴とするメモリカード。

【請求項２１】　上記請求項１～９の何れか１項に記載の各手段を構成するプログラムをコンピュータが読み出し可能に格納したことを特徴とする記憶媒体。

【請求項２２】　上記請求項１０～１８の何れか１項に記載の画像処理方法を実行するプログラムをコンピュータが読み出し可能に格納したことを特徴とする記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は画像処理システム、画像処理方法、メモリカード及び記憶媒体に関し、さらに詳しくは、電子署名を施すことで画像ファイルデータの信頼性を向上させることが可能な画像処理システム及び画像処理方法に関する。

【０００２】

【従来の技術】

従来、パーソナルコンピュータ（以下、ＰＣと省略）、電子手帳、デジタルカメラ等で作成したデータをメモリ媒体に転送して保存した後、そのメモリ媒体を画像制御装置に接続することにより、容易に印刷を実行できるようにした画像処理システム及び画像処理方法が実用化されている。

【０００３】

このデータには、出力したい画像ファイルデータの他に、どの画像をどのような出力スペックで出力を行うかを記述したプロパティファイルが含まれている。

【０００４】

図６は、特開平１０－２２６１１７号公報で開示された画像処理システムに関するものである。この画像処理システムは、画像入出力部本体６１と、画像入出

力制御装置６２と、画像入出力指令キー６３と、メモリカードI/F部６４と、メモリカード６５とを備えている。

【０００５】

上記画像入出力制御装置６２は、メモリカード６５に記憶されている画像ファイルデータのうち、どのデータを画像入出力部本体６１に転送してどのような出力スペツクで画像出力を行うかを記述したプロパティファイル及び該当画像ファイルデータをメモリカード６５から読み出して画像出力を実行するように成されている。

【０００６】

【発明が解決しようとする課題】

しかしながら、従来のこのような画像出力方法では、メモリカードに保存された画像ファイルデータが改ざん・偽造されても、それが元来のデータなのか、それとも改ざん・偽造されたデータのなのかを区別・検証することができないという問題があった。

【０００７】

また、メモリカードが第三者の手に渡った場合、それらのデータを勝手に利用することが可能であるという問題もあった。つまり、メモリカード内のデータのセキュリティー性が欠如しており、データの信頼性を保証できない問題があった。

【０００８】

本発明は上述の問題点にかんがみ、メモリ媒体内の画像ファイルデータの改ざん・偽造を判別できるようにして、メモリ媒体からの画像出力の信頼性を向上させることを目的とする。

【０００９】

【課題を解決するための手段】

上記目的を達成するために、本発明の画像処理システムは、メモリ媒体にアクセス可能なインターフェースを備えた画像処理システムであって、上記メモリ媒体に蓄積されている画像ファイルデータに関する電子署名、上記電子署名に用いた秘密鍵、または上記秘密鍵と対となる公開鍵を、上記画像ファイルデータ及び

プロパティファイルとともに読み出して記憶手段に格納する情報読み出し手段と、上記情報読み出し手段によって読み出された情報に基づいて画像の出力を行う画像出力制御手段とを具備することを特徴としている。

また、本発明の画像処理システムの他の特徴とするところは、上記情報読み出し手段によって読み出された上記画像ファイルデータに関する電子署名を、上記記憶手段に格納された公開鍵を用いて復号化する電子署名復号化手段を具備することを特徴としている。

また、本発明の画像処理システムのその他の特徴とするところは、上記画像ファイルデータから得られる画像ファイル固有のメッセージダイジェスト値を、一方向性関数を用いて算出するメッセージダイジェスト値算出手段を具備することを特徴としている。

また、本発明の画像処理システムのその他の特徴とするところは、上記画像ファイルデータの電子署名を復号化する電子署名復号化手段と、上記電子署名復号化手段によって得られるデータ値と上記メッセージダイジェスト値とを比較する比較手段と、上記比較手段の比較結果に基づいて、上記画像ファイルデータの検証を行う画像ファイルデータ検証手段とを具備することを特徴としている。

また、本発明の画像処理システムのその他の特徴とするところは、メモリ媒体にアクセス可能なインターフェースを備えた画像処理システムであって、上記インターフェースに対する上記メモリ媒体の接続を検出するメモリ媒体検出手段と、上記メモリ媒体検出手段により上記メモリ媒体の接続が検出された場合に、上記メモリ媒体に蓄積されている画像ファイルデータに関する電子署名、上記電子署名に用いた秘密鍵、またはその対となる公開鍵を、上記画像ファイルデータ及びプロパティファイルとともに転送する情報読み出し手段と、上記情報読み出し手段よって読み出された情報に基づいて画像出力を行うように制御する画像出力制御手段とを具備することを特徴としている。

また、本発明の画像処理システムのその他の特徴とするところは、メモリ媒体にアクセス可能なインターフェースを備えた画像処理システムであって、上記メモリ媒体に保存する画像ファイルデータを作成する画像ファイルデータ作成手段と、上記画像ファイルデータ作成手段によって作成された画像ファイルデータを

記憶手段に保存する画像ファイルデータ保存手段と、上記画像ファイルデータから得られる画像ファイル固有のメッセージダイジェスト値を、一方向性関数を用いて算出するメッセージダイジェスト値算出手段と、

上記メッセージダイジェスト値算出手段により算出されたメッセージダイジェスト値を、上記記憶手段内に格納された秘密鍵で暗号化するデジタル署名生成手段とを具備することを特徴としている。

また、本発明の画像処理システムのその他の特徴とするところは、上記デジタル署名生成手段によって作成されたデジタル署名をプロパティファイルに格納するデジタル署名格納手段と、上記デジタル署名が格納されたプロパティファイルを上記メモリ媒体内のプロパティ領域に保存する第１の保存手段と、上記メモリ媒体内の画像ファイル領域に署名対象画像ファイルデータを保存する第２の保存手段とを具備することを特徴としている。

また、本発明の画像処理システムのその他の特徴とするところは、上記メッセージダイジェスト値を暗号化するための秘密鍵は機器固有の秘密鍵であることを特徴としている。

また、本発明の画像処理システムのその他の特徴とするところは、上記メッセージダイジェスト値を暗号化するための秘密鍵をユーザ定義により新規に作成する秘密鍵作成手段を具備することを特徴としている。

【００１０】

本発明の画像処理方法は、メモリ媒体にアクセス可能なインターフェースを備えた画像処理システムにおける画像処理方法であって、上記メモリ媒体に蓄積されている画像ファイルデータに関する電子署名、上記電子署名に用いた秘密鍵、または上記秘密鍵と対となる公開鍵を、上記画像ファイルデータ及びプロパティファイルとともに読み出して記憶手段に格納する情報読み出し処理と、上記情報読み出し処理によって読み出された情報に基づいて画像の出力を行う画像出力制御処理とを行うことを特徴としている。

また、本発明の画像処理方法の他の特徴とするところは、上記情報読み出し処理によって読み出された上記画像ファイルデータに関する電子署名を、上記記憶手段に格納された公開鍵を用いて復号化する電子署名復号化処理を行うことを特

徴としている。

また、本発明の画像処理方法のその他の特徴とするところは、上記画像ファイルデータから得られる画像ファイル固有のメッセージダイジェスト値を、一方向性関数を用いて算出するメッセージダイジェスト値算出処理を行うことを特徴としている。

また、本発明の画像処理方法のその他の特徴とするところは、上記画像ファイルデータの電子署名を復号化する電子署名復号化処理と、上記電子署名復号化処理によって得られるデータ値と上記メッセージダイジェスト値とを比較する比較処理と、上記比較処理の比較結果に基づいて、上記画像ファイルデータの検証を行う画像ファイルデータ検証処理とを行うことを特徴としている。

また、本発明の画像処理方法のその他の特徴とするところは、メモリ媒体にアクセス可能なインターフェースを備えた画像処理システムにおける画像処理方法であって、上記インターフェースに対する上記メモリ媒体の接続を検出するメモリ媒体検出処理と、上記メモリ媒体検出処理により上記メモリ媒体の接続が検出された場合に、上記メモリ媒体に蓄積されている画像ファイルデータに関する電子署名、上記電子署名に用いた秘密鍵、またはその対となる公開鍵を、上記画像ファイルデータ及びプロパティファイルとともに転送する情報読み出し処理と、上記情報読み出し処理よって読み出された情報に基づいて画像出力を行うように制御する画像出力制御処理とを行うことを特徴としている。

また、本発明の画像処理方法のその他の特徴とするところは、メモリ媒体にアクセス可能なインターフェースを備えた画像処理システムにおける画像処理方法であって、上記メモリ媒体に保存する画像ファイルデータを作成する画像ファイルデータ作成処理と、上記画像ファイルデータ作成処理によって作成された画像ファイルデータを記憶手段に保存する画像ファイルデータ保存処理と、上記画像ファイルデータから得られる画像ファイル固有のメッセージダイジェスト値を、一方向性関数を用いて算出するメッセージダイジェスト値算出処理と、上記メッセージダイジェスト値算出処理により算出されたメッセージダイジェスト値を、上記記憶手段内に格納された秘密鍵で暗号化するデジタル署名生成処理とを行うことを特徴としている。

また、本発明の画像処理方法のその他の特徴とするところは、上記デジタル署名生成処理によって作成されたデジタル署名をプロパティファイルに格納するデジタル署名格納処理と、上記デジタル署名が格納されたプロパティファイルを上記メモリ媒体内のプロパティ領域に保存する第１の保存処理と、上記メモリ媒体内の画像ファイル領域に署名対象画像ファイルデータを保存する第２の保存処理とを行うことを特徴としている。

また、本発明の画像処理方法のその他の特徴とするところは、上記メッセージダイジェスト値を暗号化するための秘密鍵は機器固有の秘密鍵であることを特徴としている。

また、本発明の画像処理方法のその他の特徴とするところは、上記メッセージダイジェスト値を暗号化するための秘密鍵をユーザ定義により新規に作成する秘密鍵作成処理を行うことを特徴としている。

【００１１】

本発明のメモリカードは、電子署名が施された画像ファイルデータが格納されていることを特徴としている。

また、本発明のメモリカードの他の特徴とするところは、画像ファイルデータと、上記画像ファイルデータに関する電子署名と、上記電子署名に用いた秘密鍵と、上記秘密鍵と対となる公開鍵と、上記画像ファイルに係わるプロパティファイルとが格納されていることを特徴としている。

【００１２】

本発明の記憶媒体は、上記記載の各手段を構成するプログラムをコンピュータから読み出し可能に格納したことを特徴としている。

また、本発明の記憶媒体の他の特徴とするところは、上記画像処理方法を実行するプログラムをコンピュータから読み出し可能に格納したことを特徴としている。

【００１３】

【発明の実施の形態】

次に、本発明画像処理システム、画像処理方法、メモリカード及び記憶媒体の実施の形態を、図面を参照しながら説明する。

（第１の実施の形態）

図１は、第１の実施形態における画像処理システムの全体構成を示すブロック図である。図１に示したように、この画像処理システムはリーダ部（画像入力装置）２００と、プリンタ部（画像出力装置）３００とで構成されている。

【００１４】

リーダ部（画像入力装置）２００は、原稿画像を光学的に読み取り、画像データに変換するものであり、原稿を読み取るための機能を持つスキャナユニット２１０と、原稿用紙を搬送するための機能を持つ原稿給紙ユニット２５０とで構成されている。

【００１５】

また、プリンタ部（画像出力装置）３００は、記録紙を搬送し、その上に画像データを可視画像として印字して装置外に排紙するものであり、複数種類の記録紙カセットを持つ給紙ユニット３１０と、画像データを記録紙に転写、定着させる機能を持つマーキングユニット３２０と、印字された記録紙をソート、ステイプルして機外へ出力する機能を持つ排紙ユニット３３０とで構成されている。

【００１６】

また、本実施形態の画像処理システム１００は、メモリカードインターフェース（I/F）部２７０と、制御装置１１０とを具備しており、メモリカードインターフェース（I/F）部２７０は、メモリカード２７５に蓄積されているデータを読み取ったり、制御装置１１０の記憶手段１１１に蓄積されているデータをメモリカード２７５に書き込んだりする。

【００１７】

また、制御装置１１０は、リーダ部２００、プリンタ部３００、メモリカード（I/F）部２７０と電気的に接続され、さらにネットワーク４００を介して、ホストコンピュータ４０１，４０２と接続されている。

【００１８】

さらに、上記制御装置１１０は、ＣＰＵ、ＲＯＭ、ＲＡＭ等からなるコンピュータシステムにより構成されており、本実施形態の情報読み出し手段、画像出力制御手段、電子署名復号化手段、メッセージダイジェスト値算出手段、電子署名

復号化手段、比較手段、画像ファイルデータ検証手段、メモリ媒体検出手段、画像ファイルデータ作成手段、画像ファイルデータ保存手段、デジタル署名生成手段、デジタル署名格納手段、第１の保存手段、第２の保存手段及び秘密鍵作成手段等が上記コンピュータシステムのプログラムによって構成されている。

【００１９】

上述のような各手段を構成する制御装置１１０は、リーダ部２００を制御して、原稿の画像データを読込み、プリンタ部３００を制御して画像データを記録用紙に出力してコピー機能を提供する。

【００２０】

また、リーダ部２００やメモリカード（I/F）部２７０から読み取った画像データをコードデータに変換し、ネットワーク４００を介してホストコンピュータへ送信するスキャナ機能、ホストコンピュータからネットワーク４００を介して受信したコードデータを画像データに変換し、プリンタ部３００に出力するプリンタ機能を提供する。

【００２１】

操作部１５０は、制御装置１１０に接続され、液晶タッチパネルで構成され、画像処理システムを操作するためのユーザ（Ｉ／Ｆ）を提供する。

【００２２】

図２は、リーダ部２００及びプリンタ部３００の概略構成を示す断面図である。リーダ部２００の原稿給送ユニット２５０は、原稿を先頭順に１枚ずつプラテンガラス２１１上へ給送し、原稿の読み取り動作終了後、プラテンガラス２１１上の原稿を排出するものである。

【００２３】

上記制御装置１１０は、原稿がプラテンガラス２１１上に搬送されると、ランプ２１２を点灯する。また、光学ユニット２１３の移動を開始させて、原稿を露光走査する。この時の原稿からの反射光は、ミラー２１４，２１５，２１６、及びレンズ２１７によってＣＣＤイメージセンサ（以下、ＣＣＤという）２１８へ導かれる。

【００２４】

このように、走査された原稿の画像はＣＣＤ２１８によって読み取られる。ＣＣＤ２１８から出力される画像データは、所定の処理が施された後、制御装置１１０へ転送される。

【００２５】

プリンタ部３００のレーザドライバ３２１は、レーザ発光部３２２を駆動するものであり、制御装置１１０から出力された画像データに応じたレーザ光をレーザ発光部３２２により発光させる。

【００２６】

このレーザ光は、感光ドラム３２３に照射され、感光ドラム３２３にはレーザ光に応じた潜像が形成される。この感光ドラム３２３の潜像の部分には現像器３２４によって現像剤が付着される。

【００２７】

そして、レーザ光の照射開始と同期したタイミングで、カセット３１１及びカセット３１２のいずれかから記録紙を給紙して転写部３２５へ搬送し、感光ドラム３２３に付着された現像剤を記録紙に転写する。現像剤の乗った記録紙は定着部３２６に搬送され、この定着部３２６の熱と圧力により現像剤は記像紙に定着される。

【００２８】

定着部３２６を通過した記録紙は、次に排出ローラ３２７によって排出される。排紙ユニット３３０は、排出された記録紙を束ねて記録紙の仕分けをしたり、仕分けされた記録紙のステイプルを行う。

【００２９】

また、両面記録が設定されている場合は、排出ローラ３２７のところまで記録紙を搬送した後、排出ローラ３２７の回転方向を逆転させ、フラッパ３２８によって再給紙搬送路３２９へ導く。再給紙搬送路３２９へ導かれた記録紙は上述したタイミングで転写部３２５へ給紙される。

【００３０】

上述のように構成された画像処理システムにおいて、本実施形態ではメモリカード内の画像ファイルデータに電子署名を施すことで、メモリカード内の画像フ

ファイルデータの信頼性を向上させるようにしている。この電子署名技術として現在、ＲＳＡ（Rivest#Shamir#Adelman）方式などの、いわゆる非対称公開鍵方式を利用したものが知られている。上記非対称公開鍵方式は、「公開鍵」と「秘密鍵」という一対の鍵情報を設定している。

【００３１】

図３及び図４は、上記電子署名について概念的に説明したものである。この技術においては、図４中の「メッセージダイジェスト値」と「公開鍵」がポイントとなっている。上記メッセージダイジェスト値は、個々のメッセージに対し固有の値を持っている。

【００３２】

まず、署名したいデータ（テキストやバイナリ）に対して、メッセージダイジェスト値を算出する。上記メッセージダイジェスト値は、一方向性関数（ハッシュ関数）を用いて、署名したいデータから作成されるものであり、データに固有の値である。そして、上記のように作成されたメッセージダイジェスト値を秘密鍵で暗号化する。

【００３３】

電子的データの送受信を行う場合、送信側は上記秘密鍵で暗号化されたメッセージダイジェスト値を署名として、署名対象データとともに受信側に送り出す。受信側は、受信した署名データを署名側の公開鍵で復号化してメッセージダイジェスト値を得る。

【００３４】

そして、受信した署名対象データから算出されるメッセージダイジェスト値と、上記復号化したメッセージダイジェスト値とを比較する。上記のような手順で署名の検証を行うことにより電子署名が実現されている。

【００３５】

図７は、メモリカード２７５のメモリマップの一例を示す図であり、画像ファイルデータ及びプロパティファイルが保存されている。プロパティファイルは、基本的に基本的にＡＳＣＩＩコードのみで使用したText形式により記載されており、プリントジョブごとに指定情報が完結する記述となっている。また、プロパ

ティファイルはメモリカード内に１つ存在し、対象となる画像ファイルデータは保存場所を問わない。さらに、このプロパティファイルは、対象装置以外書き込み不可と設定可能なデータ記憶領域を持つ。

【００３６】

次に、上記構成からなる第１の実施形態に係わるメモリカードを利用した画像ファイルデータ改ざん防止方法を備えた画像処理システムの制御手順の一例について、図１及び図２の装置構成図及び図１０のフローチャートを用いて説明する。

【００３７】

本実施形態では、図５に示すように、ＭＤ５と呼ばれるハッシュ関数を用いて署名したいデータのメッセージダイジェスト値を算出するようにしている。上記ＭＤ５は、暗号化プログラムの１つであるＰＧＰ（Pretty Good Privacy）で現在実際に使われているメッセージダイジェスト関数である。

【００３８】

本実施形態に係わる画像処理システムでは、図７のメモリマップを有するメモリカード２７５がメモリカード（I/F）部２７０と接続された状態で制御が行われる。この時のプロパティファイルのプリントジョブ記述例は、図８のように「pic1.jpg,A4,SS,1p」となっており、それぞれ出力ファイル名＝“pic1.jpg”、出力紙サイズ＝“Ａ４”、片面印刷、出力部数＝１枚、という指定となっている。

メモリカード２７５内の画像ファイルデータを出力させる場合、ユーザは操作部１５０のメモリカード内画像データ出力キーを押下することにより、画像データファイルの検証・出力制御が開始される。

【００３９】

制御装置１１０は、メモリカード（I/F）部２７０を介してメモリカード２７５に、画像処理システムにて出力するデータが蓄積されているかどうか確認する（ステップＳ１００１）。例えば、メモリカード２７５内には、図７のメモリマップに示すように、２つの画像ファイルデータ(pic1.jpgとpic2.jpg)、画像ファイルデータpic1の署名(pic1.asc)、公開鍵(publickey.asc)、そしてプロパティ

ファイル（autprint.mrk）とが蓄積されており、それらのデータをメモリカード（I/F）部２７０を介して制御装置１１０に転送する（ステップＳ１００２）。データが蓄積されてない場合は、この制御を終了する。

【００４０】

次に、制御装置１１０は、転送された各画像ファイルデータについて対応する画像に関する電子署名が存在するか確認する（ステップＳ１００３）。この例では、pic1. Ascがpic1.jpgの電子署名となる。電子署名が存在しなければ、その画像ファイルデータには電子署名が施されていないと判断し、暗号検証の処理を行わずプロパティファイルに記述されたプリントジョブ情報に基づいて画像を出力する。

【００４１】

一方、電子署名が存在するならば、その電子署名を復号化するための公開鍵が画像処理システムに存在するか否かを確認し（ステップＳ１００４）、公開鍵が存在しないなければ操作部に「公開鍵が滞在しない」というメッセージを表示させる。この時、ユーザは暗号検証をせずにプロパティファイルに記述されたプリントジョブ情報に基づいて画像を出力するか、この制御を終了するかのどちらかを、操作部１５０において選択・指示する。

【００４２】

公開鍵が存在するならば（この例であれば、publickey.asc）、それを用いて電子署名からメッセージダイジェスト値を算出する（ステップＳ１００５）。また、画像ファイルデータからもメッセージダイジェスト値を算出し（ステップＳ１００６）、この２つのＭＤ値を検証する（ステップＳ１００７）。

【００４３】

上記検証の結果が合致すれば、この画像ファイルデータは改ざんされていないと判定でき、プロパティファイルに記述されたプリントジョブ情報に基づいて画像出力処理を行う（ステップＳ１００９）。

【００４４】

また、上記判定の結果、合致しなければ、この画像ファイルデータは改ざんされたものと判定できるので、操作部に「署名不一致」というエラーメッセージを

表示させる。

【００４５】

ユーザは、改ざんされた画像をプロパティファイルに記述されたプリントジョブ情報に基づいて出力するか、もしくはこの制御を終了するかを操作部１５０において選択・指示し（ステップＳ１００８）、その後、この制御を終了する。

【００４６】

(第２の実施の形態)

上述した第１の実施形態では、ユーザの指示によりメモリカード内の画像ファイルデータを出力する方法を述べたが、第２の実施形態では、メモリカード内のプロパティファイルに上記第１の実施形態でユーザに委ねる選択を記述し、操作部１５０のメモリカード内画像データ出力キーの押下、もしくは制御装置１１０によるメモリカード(I/F)部２７０へのメモリカード２７５の挿入検出により、上記選択された指示通り制御を行う方法について、図１，２の装置構成図、及び図１１のフローチャートを用いて説明する。

【００４７】

本実施の形態に係わる画像処理システムでは、第１の実施形態と同様に、図７のメモリマップを有するメモリカード２７５がメモリカード(I/F)部２７０と接続された状態で制御が行われる。この時のプロパティファイルのプリントジョブ記述例は、図９のように「pic1.jpg , A4, SS, 1P, NK1, UM0」となっており、それぞれ出力ファイル名＝“pic1.jpg”、出力紙サイズ＝“Ａ４”、片面印刷、出力部数＝１枚、公開鍵が不存在の時＝出力する、署名検証不一致の時＝出力しない、という指定となっている。

【００４８】

メモリカード２７５内の画像ファイルデータを出力させる場合、ユーザは操作部１５０のメモリカード内画像データ出力キーを押下、もしくは制御装置１１０によるメモリカード(I/F)部２７０へのメモリカード２７５の挿入検出により画像データファイルの検証・出力制御が開始される。

【００４９】

制御装置１１０は、メモリカード(I/F)部２７０を介してメモリカード２５０

に、画像処理システムにて出力するデータが蓄積されているかどうか確認し（ステップＳ１１０１）、蓄積されていればそれらのデータをメモリカード（I/F）部２７０を介して制御装置１１０に転送する（ステップＳ１１０２）。一方、データが蓄積されてない場合は、この制御を終了する。

【００５０】

次に、制御装置１１０は、転送された各画像ファイルデータについて対応する画像に関する電子署名が存在するか確認する（ステップＳ１１０３）。この例では、pic１．AccがpicＩjpgの電子署名となる。

【００５１】

電子署名が存在しなければその画像ファイルデータには電子署名が施されていないと判断し、暗号検証の処理を行わずプロパティファイルに記述されたプリントジョブ情報に基づいて画像を出力する（ステップＳ１１０９）。

【００５２】

電子署名が存在するならば、その電子署名を復号化するための公開鍵が画像処理システムに存在するか確認し（ステップＳ１１０４）、公開鍵が存在しないなければ操作部に「公開鍵が存在しない」というメッセージを表示させ、暗号検証をせずにプロパティファイルに記述されたプリントジョブ情報に基づいて画像を出力するか、この制御を終了するかを、プロパティファイルに記述された制御方法（図９の場合だと、出力する）に基づいて制御を行う。

【００５３】

公開鍵が存在するならば、それを用いて電子署名からメッセージダイジェスト値を算出し（ステップＳ１１０５）、また、画像ファイルデータからもメッセージダイジェスト値を算出し（ステップＳ１１０６）、この２つのＭＤ値を検証する（ステップＳ１１０７）。

【００５４】

上記検証の結果、合致すれば、該画像ファイルデータは改ざんされていないと判定でき、プロパティファイルに記述されたプリントジョブ情報に基づいて画像出力処理を行う。もし、合致しなければ、該画像ファイルデータは改ざんされたものと半淀でき、操作部に「署名不一致」というエラーメッセージを表示させる

。

【００５５】

そして、改ざんされた画像をプロパティファイルに記述されたプリントジョブ情報に基づいて出力するかもしくはこの撮脚を終了するかを、プロパティファイルに記述された制御方法（図９の場合だと、出力しない）に基づいて制御を行い（ステップＳ１１０８）、その後、この制御を終了する。

【００５６】

(第３の実施の形態)

第１の実施形態及び第２の実施形態においては、画像処理システムのメモリカード(I/F)を介してメモリカードに蓄積された画像ファイルデータの検証、出力方法に関して述べた。

【００５７】

この第３の実施形態では、画像処理システムがネットワークを介してホストコンピュータと接続されていることを利用して、ホストコンピュータのメモリカード(I/F)を介してメモリカードに蓄積されている画像ファイルデータ、画像ファイルデータの電子署名、プロパティファイルなどを画像処理システムに転送し、画像の検証・出力を行う方法について、図１，２の装置構成図、及び図１２のフローチャートを用いて説明する。

【００５８】

本実施の形態に係わる画像処理システムでは、第１の実施形態、第２の実施形態と同様に、メモリカード４０４がメモリカード(I/F)４０３と接続された状態で制御が行われる。

【００５９】

メモリカード４０４内の画像ファイルデータをホストコンピュータ４０１側で取り込み、ネットワーク４００を介して画像処理システム１００の制御装置１１０に転送して出力させる場合、ユーザはホストコンピュータ４０１を操作して制御を開始するか、もしくは、画像処理システム１００の操作部１５０においてネットワーク４００に接続されているホストコンピュータ４０１を介してメモリカード４０４内画像データを取り込み、出力するキーを押下することにより、画像

データファイルの取り込み・検証・出力制御が開始される。

【００６０】

制御装置１１０は、ネットワーク接続されているホストコンピュータ４０１のメモリカード（I/F）４０３を介してメモリカード４０４に出力するデータが蓄積されているかどうか確認し（ステップＳ１２０１）、蓄積されていればそれらのデータをメモリカード(I/F)４０３及びネットワーク４００を介して制御装置１１０に転送する（ステップＳ１２０２）。データが蓄積されてない場合は、この制御を終了する。また、該当プログラムが制御装置１１０に存在しない場合には、そのプログラムをネットワーク４００を介してホストコンピュータ４０１より制御装置１１０に転送する。

【００６１】

次に、制御装置１１０は転送された各画像ファイルデータについて対応する画像に関する電子署名が存存するか確認する（ステップＳ１２０３）。この確認の結果、電子署名が存在しなければ、その画像ファイルデータには電子署名が施されていないと判断し、暗号検証の処理を行わずプロパティファイルに記述されたプリントジョブ情報に基づいて画像を出力する（ステップＳ１２０９）。

【００６２】

一方、上記確認の結果、電子署名が存在するならば、その電子署名を復号化するための公開鍵が画像処理システムに存在するか確認（ステップＳ１２０４）し、公開鍵が存在しないならば操作部１５０もしくはホストコンピュータ４０１に「公開鍵が存在しない」というメッセージを表示させ、暗号検証をせずにプロパティファイルに記述されたプリントジョブ情報に基づいて画像を出力するかこの制御を終了するかを、操作部１５０またはホストコンピュータ４０１において選択・指示するか、もしくはプロパティファイルに記述された撮御方法（図９の場合だと、出力する）に基づいて制御を行う。

【００６３】

公開鍵が存在するならば、それを用いて電子署名からメッセージダイジェスト値を算出し（ステップＳ１２０５）、また、画像ファイルデータからもメッセージダイジェスト値を算出し（ステップＳ１２０６）、この２つのＭＤ値を検証す

る（ステップＳ１２０７）。

【００６４】

合致すれば、該画像ファイルデータは改ざんされていないと判定でき、プロパティファイルに記述されたプリントジョブ情報に基づいて画像出力処理を行う（ステップＳ１２０９）。もし合致しなければ、該画像ファイルデータは改ざんされたものと判定でき、操作部１５０またはホストコンピュータ４０１に「署名不一致」というエラーメッセージを表示させる。

【００６５】

そして、改ざんされた画像をプロパティファイルに記述されたプリントジョブ情報に基づいて出力するかもしくはこの制御を終了するかを、操作部１５０またはホストコンピュータ４０１において選択・指示するか、もしくはプロパティファイルに記述された制御方法（図９の場合だと、出力しない）に基づいて制御を行い（ステップＳ１２０８）、その後、この制御を終了する。

【００６６】

(第４の実施の形態)

第４の実施形態では、画像処理システムのリーダ部もしくはネットワークを介して接続されているホストコンピュータにより取り込まれた画像を制御装置内の秘密鍵を用いて署名し、画像ファイルデータ、その電子署名、及びプロパティファイルをメモリカードに保存する方法について説明する。

【００６７】

ある原稿を画像処理システムのリーダ部２００にて取り込み、その画像データをメモリカードに保存しようとする時、操作部１５０にてその制御の実行開始ボタン等を押下することにより、この制御が開始される。

【００６８】

まず、原稿読み取りの制御手順に関して、図２の断面図を用いて説明する。原稿がプラテンガラス２１１上に搬送されると、ランプ２１２を点灯させる。そして、光学ユニット２１３の移動を開始させて、原稿を露光走査する。この時の原稿からの反射光は、ミラー２１４，２１５，２１６、及びレンズ２１７によってＣＣＤイメージセンサ（以下ＣＣＤという）２１８へ導かれる。

【００６９】

このように、走査された原稿の画像はＣＣＤ２１８によって読み取られる。ＣＣＤ２１８から出力される画像データは、所定の処理が施された後、制御装置１１０へ転送される。

【００７０】

一方、ホストコンピュータ４０１，４０２にある画像ファイルデータをネットワーク４００を介して制御装置１１０に転送し、その画像ファイルデータをメモリカード２７５に保存しようとする時は、ホストコンピュータ４０１，４０２もしくは操作部１５０に配設されている制御開始ボタンを押下することによりこの制御が開始され、画像ファイルデータはネットワーク４００を介して画像処理システムの制御装置１１０に転送される。

【００７１】

以後の制御は、画像ファイルデータをリーダ部２００で読み取った場合と、ホストコンピュータ４０１，４０２からネットワーク４００を介して転送した場合と同様となり、図１３のフローチャートを用いて説明する。

【００７２】

制御装置１１０は、取り込んだ画像をメモリカード２７５に保存する時、電子署名を行うかどうかユーザに確認するため、操作部１５０もしくはホストコンピュータ４０１，４０２にその意向を表示して、データに電子署名を行うか否かを選択させる（ステップＳ１３０１）。

【００７３】

図１５は、この意向表示の一例であり、これに限定されるものではない。署名を行わない場合は、すぐさまメモリカード２７５にその画像ファイルデータを保存して（ステップＳ１３１１）、制御処理を終了する。

【００７４】

一方、署名を行う場合、秘密鍵を新規に作成するか否かを選択させる（ステップＳ１３０２）。この結果、秘密鍵を新規に作成する場合には秘密鍵暗証番号の入力を行い（ステップＳ１３０２）、その後、秘密鍵の作成・保存を行う（ステップＳ１３０４）。その後、公開鍵の作成・保存を行う（ステップＳ１３０５）

。

【００７５】

また、秘密鍵を新規に作成しない場合には、システムに保存された秘密鍵を選択し（ステップＳ１３０６）、公開鍵が存在するか否かを判定する（ステップＳ１３０７）。この判定の結果、存在する場合にはステップＳ１３０５に進んで公開鍵の作成・保存を行う。

【００７６】

次に、署名対象ファイルデータのメッセージダイジェスト値を算出し（ステップＳ１３０８）、上記メッセージダイジェスト値を秘密鍵で暗号化し（ステップＳ１３０９）、この暗号化されたメッセージダイジェスト値を署名としてメモリカードに保存する（ステップＳ１３１０）。

【００７７】

この秘密鍵や対となる公開鍵は、署名時にユーザ自身が新たに作成することもできるし、また、画像処理システムに保有されているもの用いることもできる。ユーザが秘密鍵を作成する場合、制御装置はユーザに対して任意の暗証番号を入力してもらうことにより自動的に秘密鍵、公開鍵を作成する。その後、署名対象となった画像ファイルデータをメモリカードに保存する（ステップＳ１３１１）。

【００７８】

次に、プリントジョブデータの作成を行うか否かを選択させるために、制御装置は操作部１５０もしくはホストコンピュータ４０１，４０２にその意向を表示する（ステップＳ１３１２）。

【００７９】

図１６は、この意向表示の一例であり、これに限定されるものではない。プリントジョブデータの作成を行う場合、ユーザま操作部において、出力用紙サイズ、枚数、オプションなどといったプリントジョブ項目を選択し、その選択したプリントジョブデータをメモリカードのプロパティファイルに保存する（ステップＳ１３１３）。

【００８０】

次に、制御装置１１０は、画像を署名する時に用いた秘密鍵やその対となる公開鍵をメモリカードに保存するかどうかユーザに確認する。図１７は、この意向表示の一例であるが、これに限定されるものではない。

【００８１】

次に、秘密鍵、公開鍵の保存、表示方法について、図１４のフローチャートを用いて説明する。

最初に、秘密鍵・公開鍵を保存、表示するか否かの選択を行わせ（ステップＳ１４００）、保存、表示を行わない場合には処理を終了する。また、処理を行う場合には、これらの鍵の保存・表示方法について選択する項目が出力装置に表示される（ステップＳ１４０２）。

【００８２】

図１８は、この意向表示の一例であり、これに限定されるものではない。特に公開鍵は、上記画像ファイルデータと上記署名との検証に用いられるため、何らかの方法で保存しておく必要がある。これらの扱いについては、以下のような選択肢がある。

【００８３】

公開鍵について、

（１）公開鍵を画像ファイルデータと署名が保存されているメモリカードと同一のメモリカードに保存する。

（２）公開鍵を画像ファイルデータと署名が保存されているメモリカードと別のメモリカードに保存する。

（３）公開鍵を操作部に表示する。

【００８４】

秘密鍵について、

（１）秘密鍵を画像ファイルデータと署名が保存されているメモリカードと同一のメモリカードに保存する。

（２）秘密鍵を画像ファイルデータと署名が保存されているメモリカードと別のメモリカードに保存する。

（３）秘密鍵を操作部に表示する。

【００８５】

上記秘密鍵、上記公開鍵の保存・表示方法を選択した結果、保存・表示を行わない場合には処理を終了する。

一方、公開鍵の保存・表示を行う場合には、ユーザに保存・表示形態について確認させる(ステップＳ１４０２)。

【００８６】

次に、署名付き画像ファイルデータを保存しているメモリカードと同一メモリカードに秘密鍵を保存するか否かを決めさせる(ステップＳ１４０３)。この判定の結果、同じメモリカードに保存しない場合にはステップＳ１４０５に進む。また、同じメモリカードに保存する場合は、画像ファイルデータが保存されているメモリカードに秘密鍵を保存する（ステップＳ１４０４）。その後、ステップＳ１４０５に進む。

【００８７】

次に、ステップＳ１４０５では、秘密鍵をデータとは別のメモリカードに保存するか否かを決定させる。この結果、秘密鍵を署名付き画像ファイルデータと別のメモリカードに保存する場合、ステップＳ１４０６に進んで秘密鍵保存フラグをオンにし、その後、ステップＳ１４０７に進む。

【００８８】

ステップＳ１４０７では、秘密鍵を表示するか否かを判定し、表示する場合にはステップＳ１４０８に進んで秘密鍵を表示する。また、表示しない場合にはステップＳ１４０９に進む。

【００８９】

ステップＳ１４０９では、署名付き画像ファイルデータを保存しているメモリカードと同一メモリカードに公開鍵を保存するか否かを決めさせる。この判定の結果、同じメモリカードに保存しない場合にはステップＳ１４１１に進む。また、同じメモリカードに保存する場合は、画像ファイルデータが保存されているメモリカードに公開鍵を保存する（ステップＳ１４１０）。その後、ステップＳ１４１１に進む。

【００９０】

次に、ステップＳ１４１１では、公開鍵をデータとは別のメモリカードに保存するか否かを決定させる。この結果、公開鍵を署名付き画像ファイルデータと別のメモリカードに保存する場合、ステップＳ１４１２に進んで公開鍵保存フラグをオンにし、その後、ステップＳ１４１３に進む。

【００９１】

ステップＳ１４１３では、公開鍵を表示するか否かを判定し、表示する場合にはステップＳ１４１４に進んで公開鍵を表示する。また、表示しない場合にはステップＳ１４１５に進む。

【００９２】

ステップＳ１４１５では、秘密鍵フラグまたは公開鍵フラグがオンになっているか否かを判定する。この判定の結果、フラグがオンになっている場合には、ステップＳ１４１６に進んでメモリカードを交換するようユーザに指示した後に、交換されたメモリカードを認識し、その後、秘密鍵をフラグがオンの鍵をメモリカードに保存する（ステップＳ１４１７）。

【００９３】

これらの秘密鍵や公開鍵、そして署名や画像ファイルデータは、ユーザの選択によりメモリカード２７５の対象装置以外の書き込み不可領域に保存することもできる（ステップＳ１４１１及びステップ１４１２）。

【００９４】

（本発明の他の実施の形態）

本発明は複数の機器（例えば、ホストコンピュータ、インターフェース機器、リーダ、プリンタ等）から構成されるシステムに適用しても１つの機器からなる装置に適用しても良い。

【００９５】

また、上述した実施の形態の機能を実現するように各種のデバイスを動作させるように、上記各種デバイスと接続された装置あるいはシステム内のコンピュータに対し、上記実施の形態の機能を実現するためのソフトウェアのプログラムコードを供給し、そのシステムあるいは装置のコンピュータ（ＣＰＵあるいはＭＰＵ）に格納されたプログラムに従って上記各種デバイスを動作させることによっ

て実施したものも、本発明の範疇に含まれる。

【００９６】

また、この場合、上記ソフトウェアのプログラムコード自体が上述した実施の形態の機能を実現することになり、そのプログラムコード自体、及びそのプログラムコードをコンピュータに供給するための手段、例えばかかるプログラムコードを格納した記憶媒体は本発明を構成する。かかるプログラムコードを記憶する記憶媒体としては、例えばフロッピーディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、磁気テープ、不揮発性のメモリカード、ＲＯＭ等を用いることができる。

【００９７】

また、コンピュータが供給されたプログラムコードを実行することにより、上述の実施の形態で説明した機能が実現されるだけでなく、そのプログラムコードがコンピュータにおいて稼働しているＯＳ（オペレーティングシステム）あるいは他のアプリケーションソフト等の共同して上述の実施の形態で示した機能が実現される場合にもかかるプログラムコードは本発明の実施の形態に含まれることは言うまでもない。

【００９８】

さらに、供給されたプログラムコードがコンピュータの機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその機能拡張ボードや機能拡張ユニットに備わるＣＰＵ等が実際の処理の一部または全部を行い、その処理によって上述した実施の形態の機能が実現される場合にも本発明に含まれる。また、上述した実施形態ではメモリ媒体としてカードを例に挙げて説明したが、上記メモリ媒体としてはカード状の媒体のみならず、例えば、スティック状のメモリ媒体であってもよく、形態はかまわない。また、上述した実施形態において、秘密鍵、公開鍵の両方あるいは一方だけを電子署名データとともに格納するようにしてもよい。

【００９９】

【発明の効果】

以上説明したように、本発明によれば、メモリ媒体に保存されている署名付き

画像ファイルデータを画像処理システムに転送し出力しようとする場合、上記画像処理システム内で一方向性関数を用いて算出される上記画像ファイルデータのメッセージダイジェスト値と、上記署名を復号する公開鍵を用いて復号化される値とを比較検討することによって、上記画像ファイルデータが改ざんされたかどうか確実に判別することが可能となり、メモリ媒体に格納した画像の信頼性を大幅に向上させることができる。

【０１００】

また、本発明の他の特徴によれば、ユーザに委ねる選択をプロパティファイルに記述することにより、ユーザはより容易に画像ファイルデータを検証・出力することができる。

【０１０１】

また、本発明のその他の特徴によれば、画像処理システムがネットワークを介してホストコンピュータと接続されていることを利用して、画像処理システム以外のメモリカード(I/F)に接続されたメモリ媒体から、画像ファイルデータを画像処理システムに転送することができ、ユーザはより容易に画像ファイルデータの出力・検証を行うことができる。

【０１０２】

また、本発明のその他の特徴によれば、リーダ部により取り込まれた画像ファイルデータやホストコンピュータにおいて作成された画像ファイルデータをメモリ媒体に保存する際に、一方向性関数を用いて上記画像ファイルデータのメッセージダイジェスト値を算出し、秘密鍵を用いて上記メッセージダイジェスト値を署名し、上記画像ファイルデータとともに上記メモリ媒体に保存するようにしたので、上記画像ファイルデータの改ざんを確実に防止することができ、上記画像ファイルデータの信頼性を向上させることができる。

【図面の簡単な説明】

【図１】

本発明の実施形態を示し、画像処理システムの概略構成を示すブロック図である。

【図２】

本発明の画像出力装置の構成を示す断面図である。

【図３】

電子署名に関する説明図である。

【図４】

電子署名に関する説明図である。

【図５】

電子的データとメッセージダイジェスト値との関連を説明する図である。

【図６】

メモリカードを画像処理システムに接続したシステムの一例を示すブロック図である。

【図７】

本発明の第１の実施形態、第２の実施形態、第３の実施形態におけるメモリカードのメモリマップの一例説明する図である。

【図８】

第１の実施形態に関するプロパティファイルスクリプトの内容の一例を示す説明図である。

【図９】

第２の実施形態に関するプロパティファイルスクリプトの内容の一例を示す説明図である。

【図１０】

第１の実施形態の処理手順を説明するフローチャートである。

【図１１】

第２の実施形態の処理手順を説明するフローチャートである。

【図１２】

第３の実施形態の処理手順を説明するフローチャートである。

【図１３】

第４の実施形態の処理手順を説明するフローチャートである。

【図１４】

第４の実施形態の処理手順を説明するフローチャートである。

【図１５】

第１の実施形態を説明する画像処理システムの操作部の表示例を示す説明図である。

【図１６】

第２の実施形態を説明する画像処理システムの操作部の表示例を示す説明図である。

【図１７】

第３の実施形態を説明する画像処理システムの操作部の表示例を示す説明図である。

【図１８】

第４の実施形態を説明する画像処理システムの操作部の表示例を示す説明図である。

【符号の説明】

１００　画像処理システム

１１０　制御装置

２００　リーダ部（画像入力装置）

３００　プリンタ部（画像出力装置）

２１０　スキャナユニット

２５０　原稿給紙ユニット

３１０給紙ユニット

３２０　マーキングユニット

３３０　排紙ユニット

２７０　メモリカードインターフェース（I/F）部

２７５　メモリカード

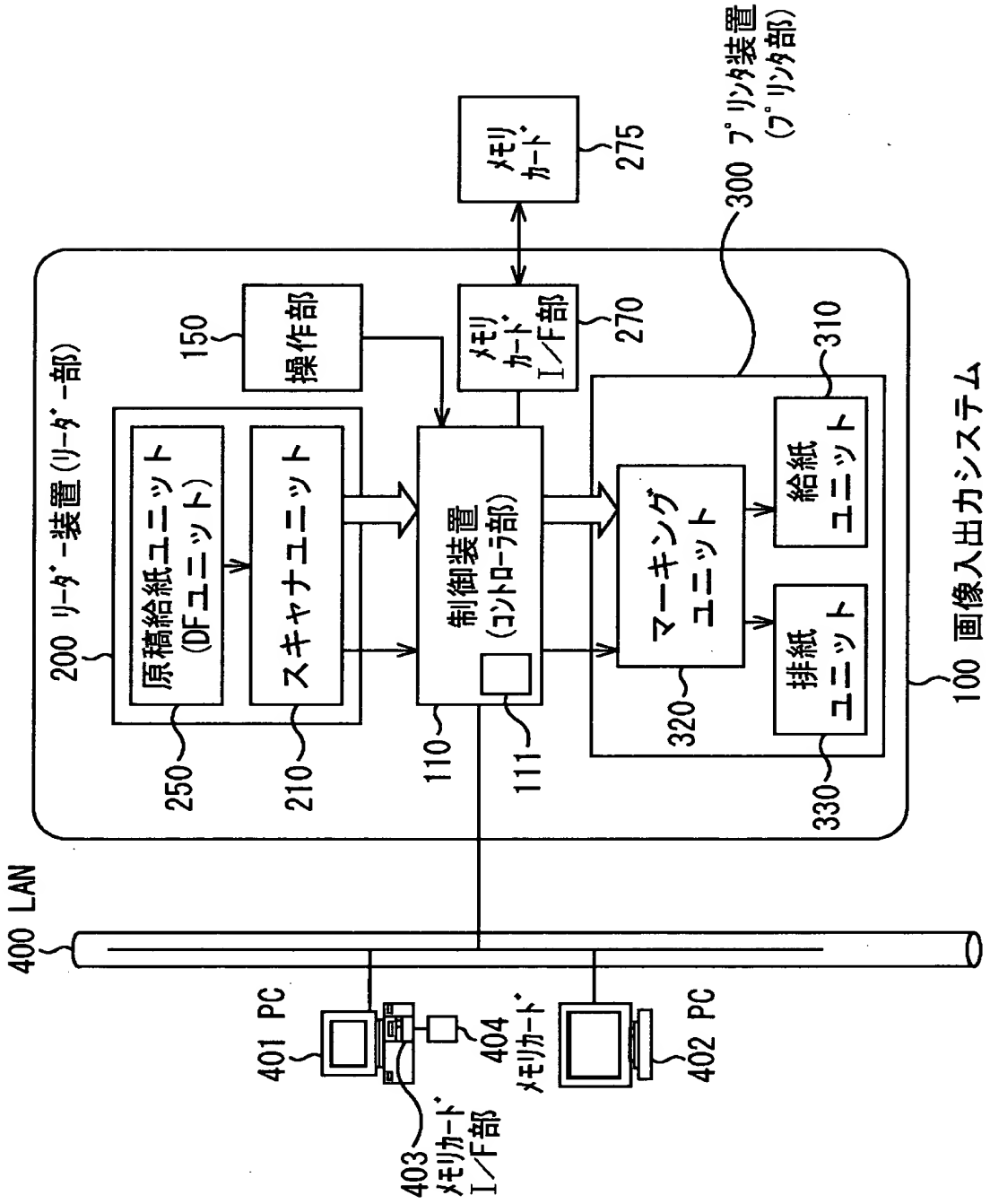
４００　ネットワーク

４０１、４０２　ホストコンピュータ

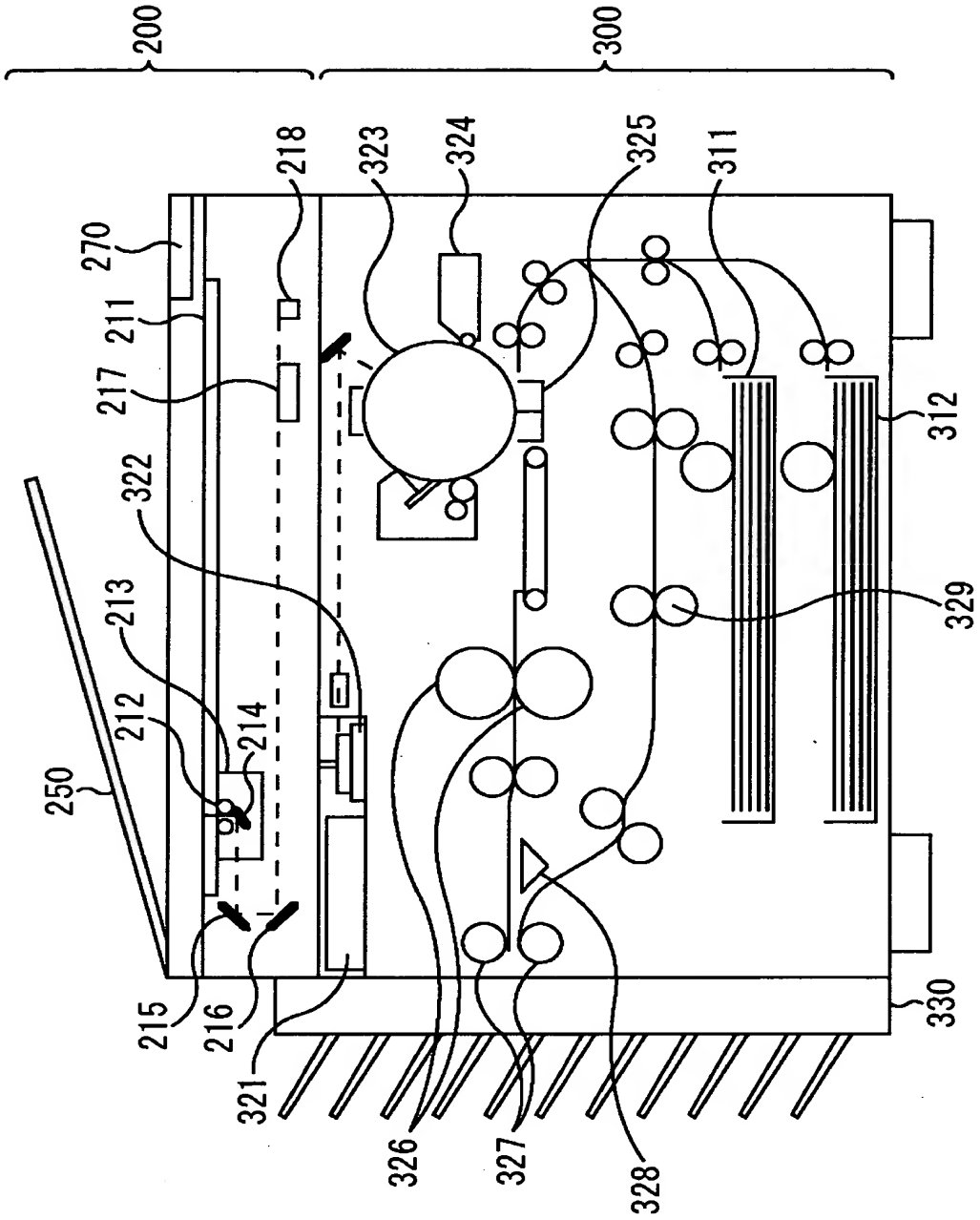
４０３　メモリカード(I/F)

【書類名】　　図面

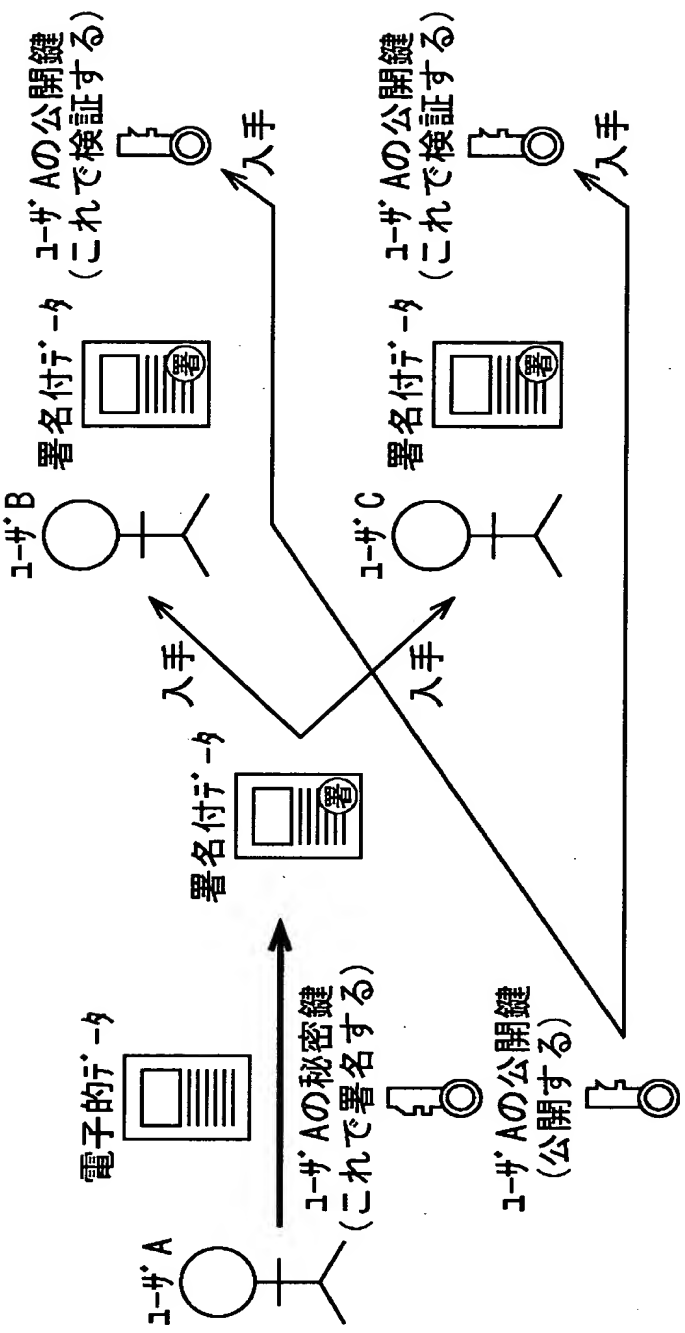
【図１】


メモリカード
275
300 プリンタ装置(プリンタ部)
150
操作部
メモリカードI/F部
270
310
200 リーダー装置(リーダー部)
原稿給紙ユニット(DFユニット)
スキャナユニット
制御装置(コントローラ部)
マーキングユニット
給紙ユニット
排紙ユニット
100 画像入出力システム
250
210
110
111
320
330
400 LAN
401 PC
403 メモリカードI/F部
404 メモリカード
402 PC

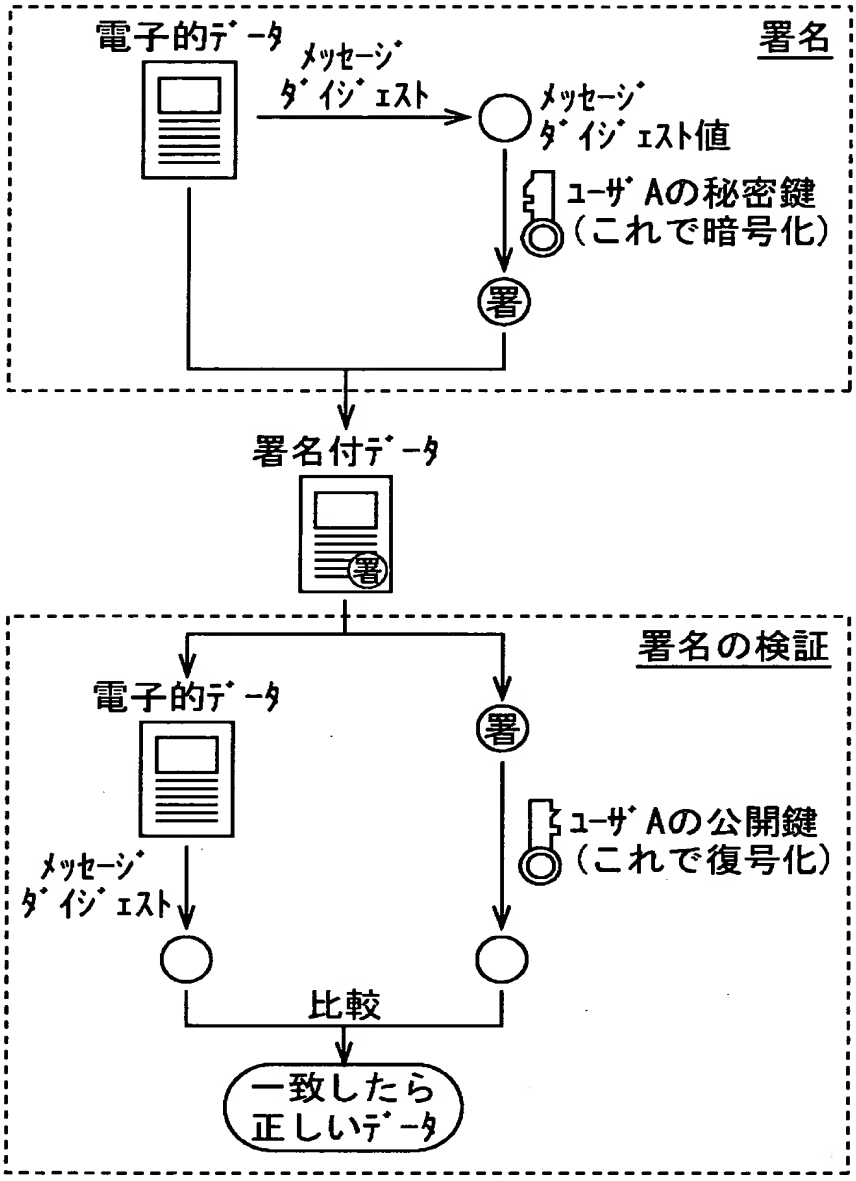
【図２】


200
300
218
323
324
325
311
270
211
217
322
213
212
214
250
312
329
330
215
216
321
326
327
328

【図３】


ユーザA
電子的データ
ユーザAの秘密鍵
（これで署名する）
署名付データ
ユーザAの公開鍵
（公開する）
入手
入手
ユーザB
署名付データ
ユーザAの公開鍵
（これで検証する）
入手
ユーザC
署名付データ
ユーザAの公開鍵
（これで検証する）
入手

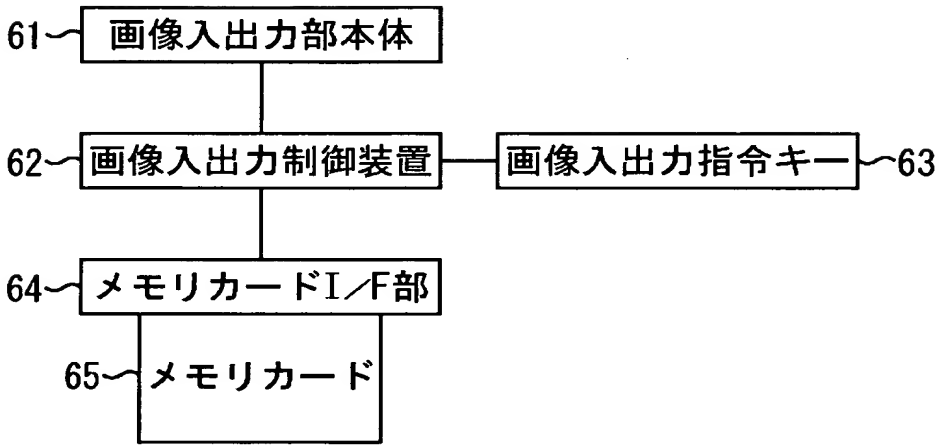
【図４】


電子的ﾃﾞｰﾀ
ﾒｯｾｰｼﾞ ﾀﾞｲｼﾞｪｽﾄ
ﾒｯｾｰｼﾞ ﾀﾞｲｼﾞｪｽﾄ値
署名
ﾕｰｻﾞAの秘密鍵 (これで暗号化)
署
署名付ﾃﾞｰﾀ
署名の検証
電子的ﾃﾞｰﾀ
署
ﾕｰｻﾞAの公開鍵 (これで復号化)
ﾒｯｾｰｼﾞ ﾀﾞｲｼﾞｪｽﾄ
比較
一致したら 正しいﾃﾞｰﾀ

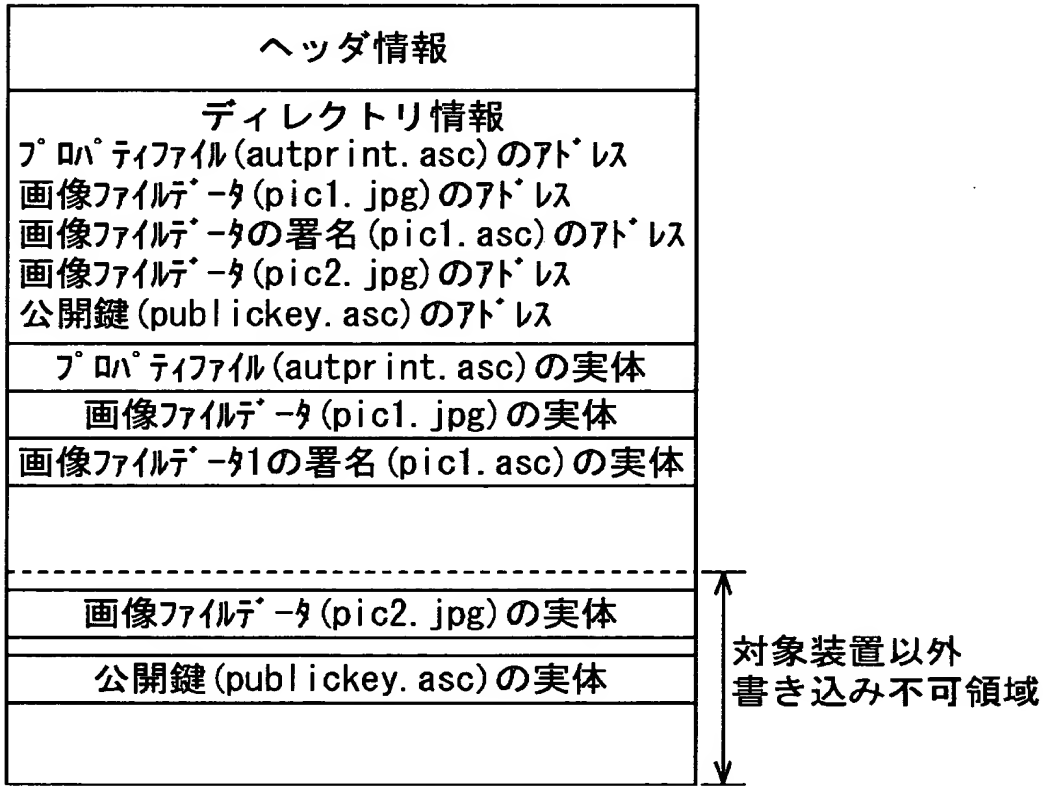
【図５】


電子的ﾃﾞｰﾀ
ﾒｯｾｰｼﾞ ﾀﾞｲｼﾞｪｽﾄ値
ハッシュ関数(MD5)

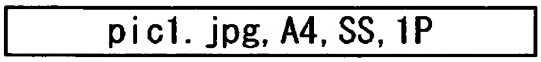
【図６】


61
画像入出力部本体
62
画像入出力制御装置
画像入出力指令キー
63
64
メモリカードI／F部
65
メモリカード

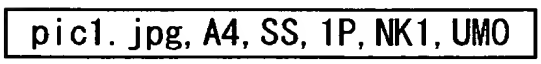
【図７】


ヘッダ情報
ディレクトリ情報
ﾌﾟﾛﾊﾟﾃｨﾌｧｲﾙ(autprint.asc)のｱﾄﾞﾚｽ
画像ﾌｧｲﾙﾃﾞｰﾀ(pic1.jpg)のｱﾄﾞﾚｽ
画像ﾌｧｲﾙﾃﾞｰﾀの署名(pic1.asc)のｱﾄﾞﾚｽ
画像ﾌｧｲﾙﾃﾞｰﾀ(pic2.jpg)のｱﾄﾞﾚｽ
公開鍵(publickey.asc)のｱﾄﾞﾚｽ
ﾌﾟﾛﾊﾟﾃｨﾌｧｲﾙ(autprint.asc)の実体
画像ﾌｧｲﾙﾃﾞｰﾀ(pic1.jpg)の実体
画像ﾌｧｲﾙﾃﾞｰﾀ1の署名(pic1.asc)の実体
画像ﾌｧｲﾙﾃﾞｰﾀ(pic2.jpg)の実体
公開鍵(publickey.asc)の実体
対象装置以外
書き込み不可領域

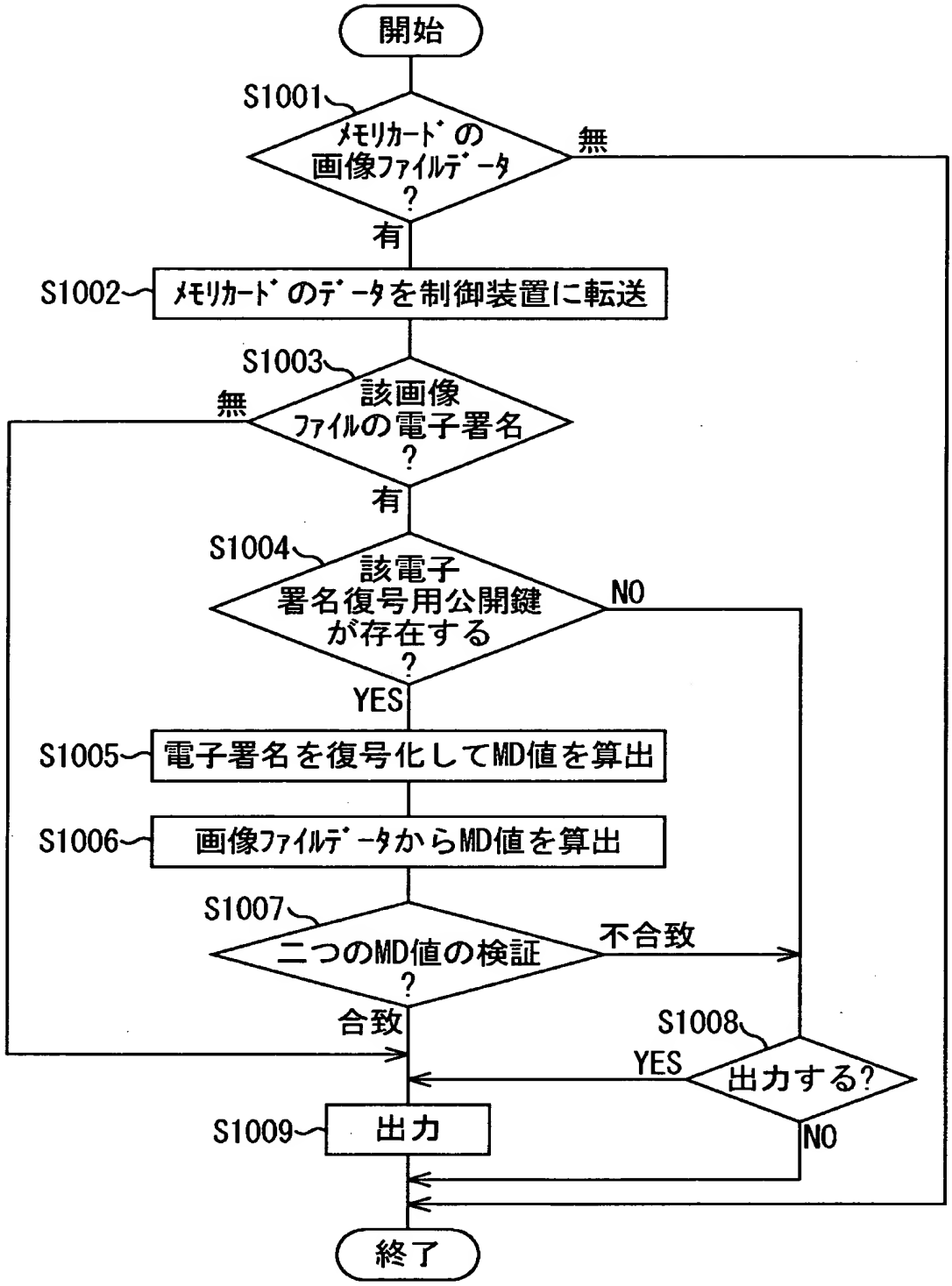
【図８】


pic1.jpg,A4,SS,1P

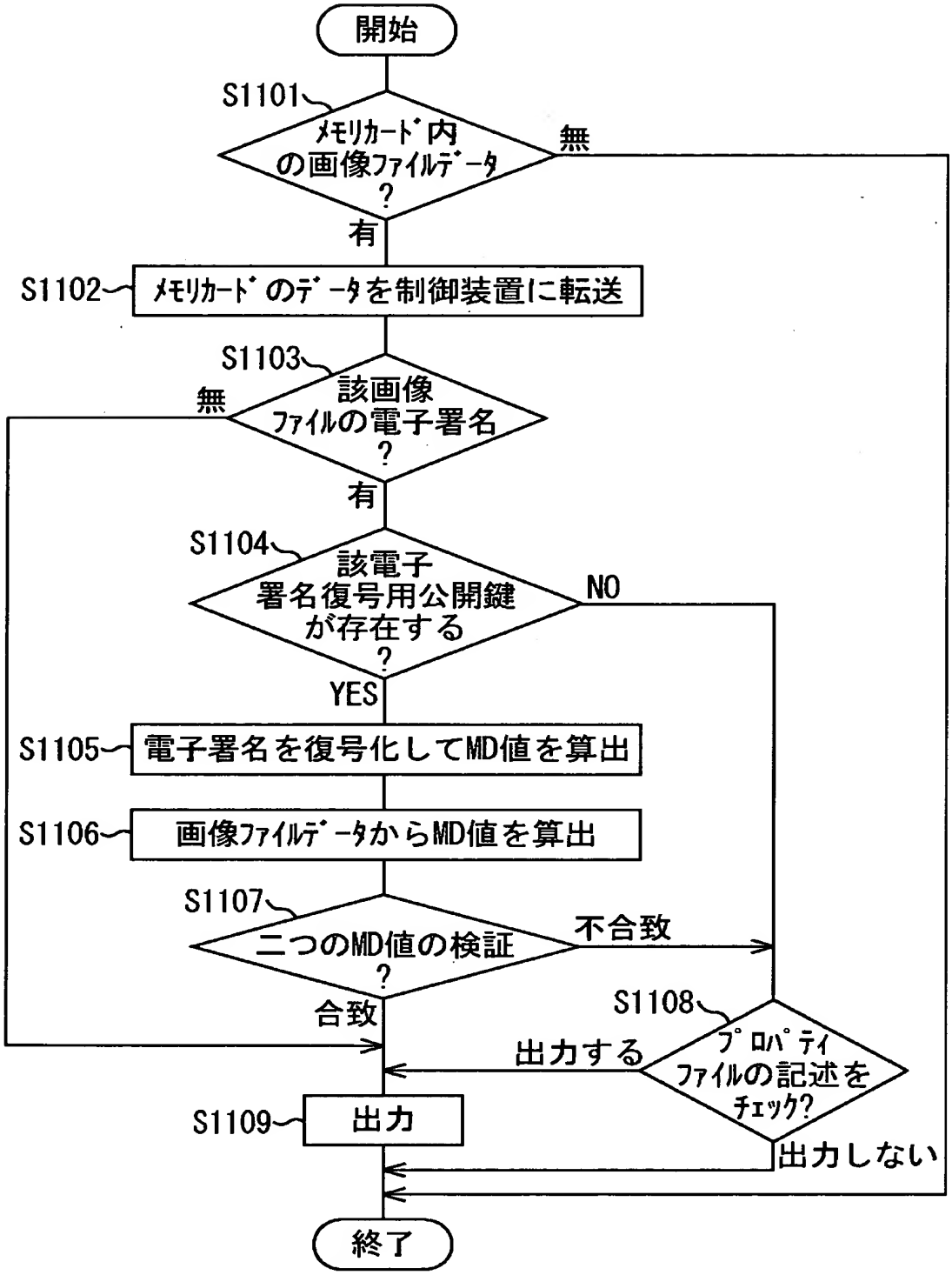
【図９】


pic1.jpg,A4,SS,1P,NK1,UMO

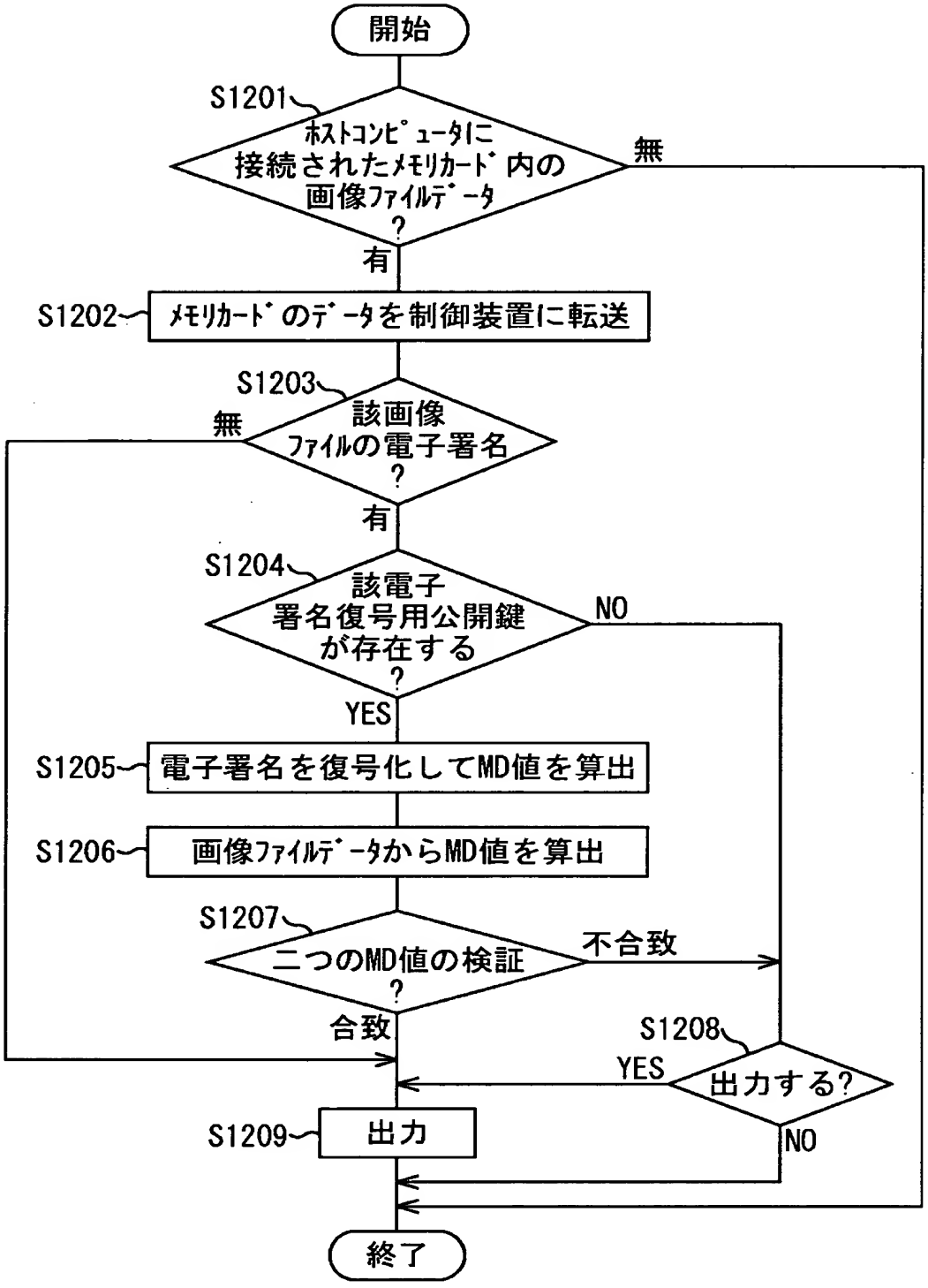
【図１０】


開始
S1001
ﾒﾓﾘｶｰﾄﾞの画像ﾌｧｲﾙﾃﾞｰﾀ？
無
有
S1002
ﾒﾓﾘｶｰﾄﾞのﾃﾞｰﾀを制御装置に転送
S1003
該画像ﾌｧｲﾙの電子署名？
無
有
S1004
該電子署名復号用公開鍵が存在する？
NO
YES
S1005
電子署名を復号化してMD値を算出
S1006
画像ﾌｧｲﾙﾃﾞｰﾀからMD値を算出
S1007
二つのMD値の検証？
不合致
合致
S1008
出力する？
YES
NO
S1009
出力
終了

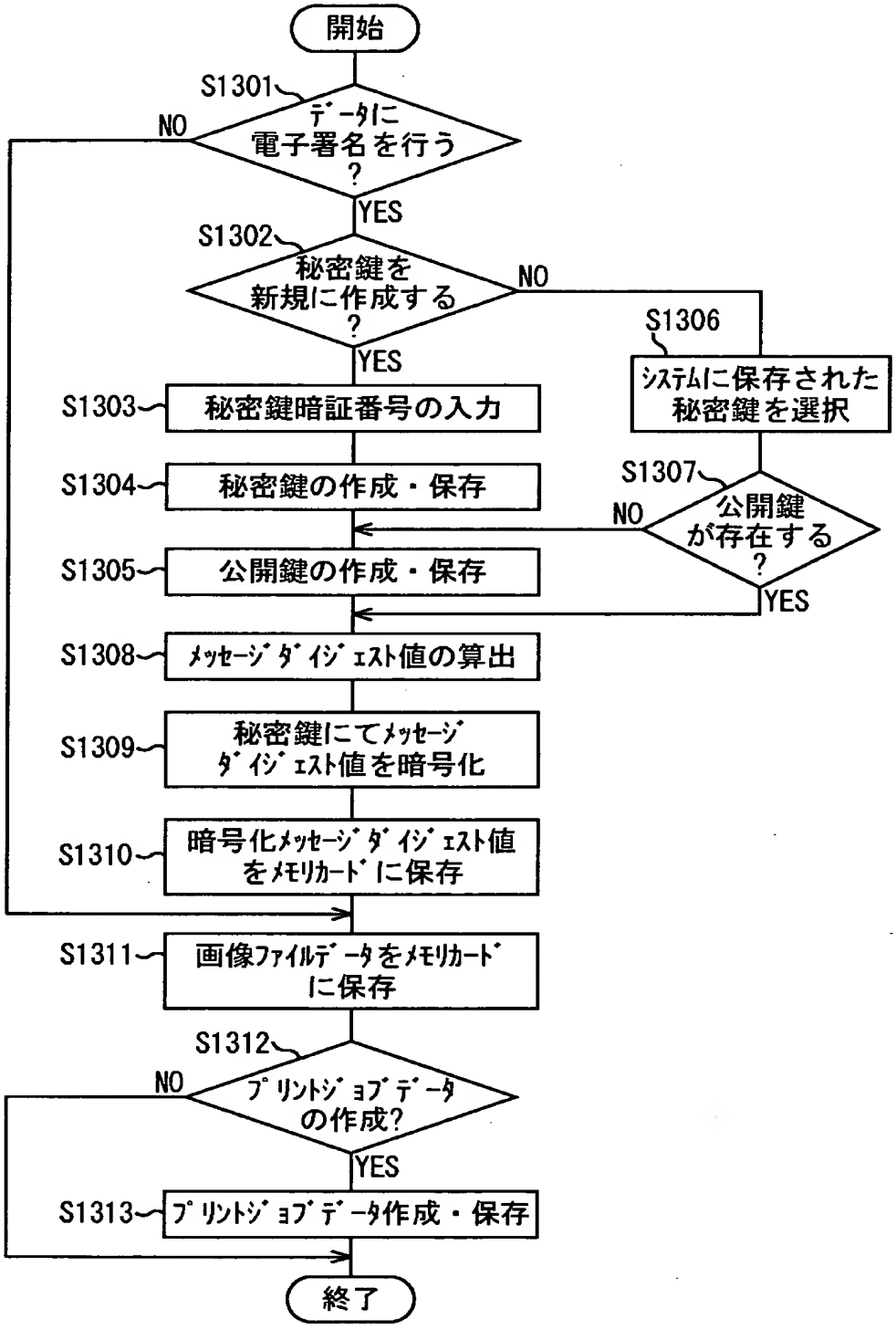
【図１１】


開始
S1101
ﾒﾓﾘｶｰﾄﾞ内の画像ﾌｧｲﾙﾃﾞｰﾀ？
無
有
S1102
ﾒﾓﾘｶｰﾄﾞのﾃﾞｰﾀを制御装置に転送
S1103
該画像ﾌｧｲﾙの電子署名？
無
有
S1104
該電子署名復号用公開鍵が存在する？
NO
YES
S1105
電子署名を復号化してMD値を算出
S1106
画像ﾌｧｲﾙﾃﾞｰﾀからMD値を算出
S1107
二つのMD値の検証？
不合致
合致
S1108
ﾌﾟﾛﾊﾟﾃｨﾌｧｲﾙの記述をﾁｪｯｸ?
出力する
出力しない
S1109
出力
終了

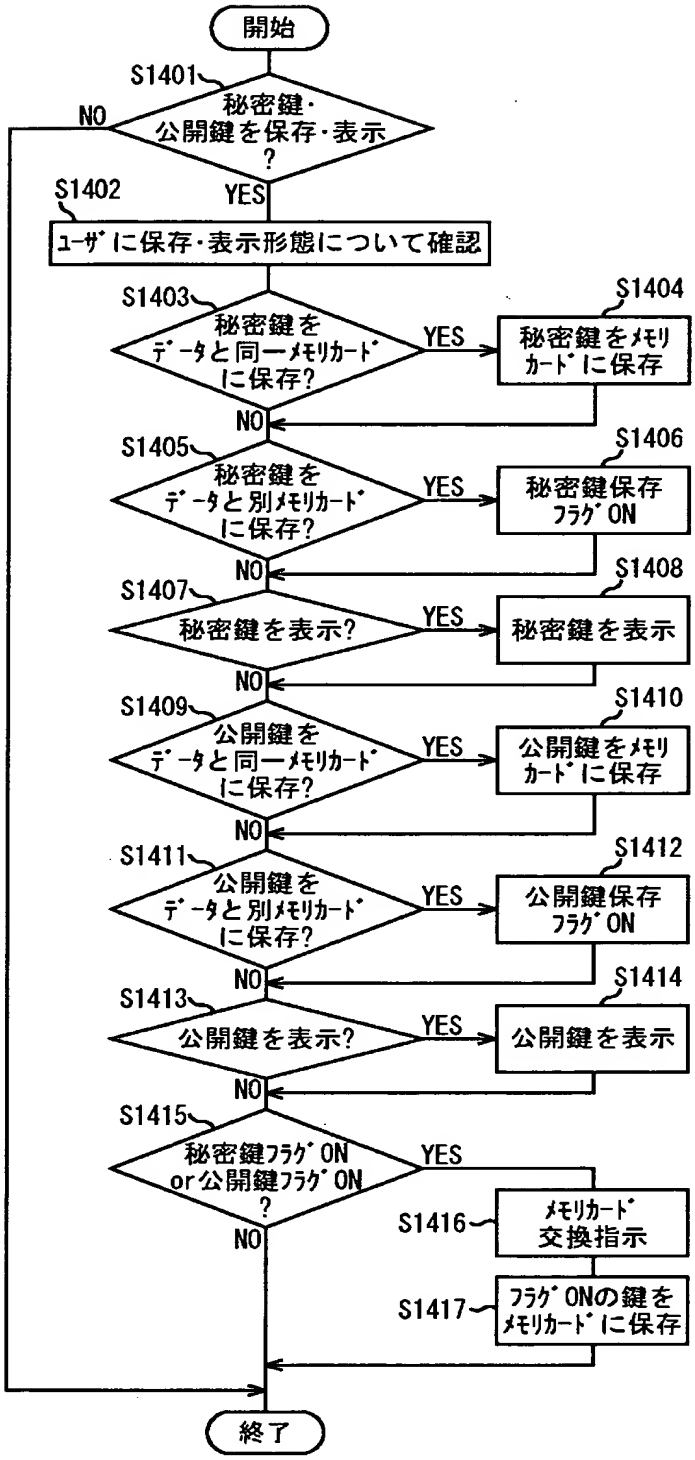
【図１２】


開始
S1201
ﾎｽﾄｺﾝﾋﾟｭｰﾀに接続されたﾒﾓﾘｶｰﾄﾞ内の画像ﾌｧｲﾙﾃﾞｰﾀ？
無
有
S1202
ﾒﾓﾘｶｰﾄﾞのﾃﾞｰﾀを制御装置に転送
S1203
該画像ﾌｧｲﾙの電子署名？
無
有
S1204
該電子署名復号用公開鍵が存在する？
NO
YES
S1205
電子署名を復号化してMD値を算出
S1206
画像ﾌｧｲﾙﾃﾞｰﾀからMD値を算出
S1207
二つのMD値の検証？
不合致
合致
S1208
出力する？
YES
NO
S1209
出力
終了

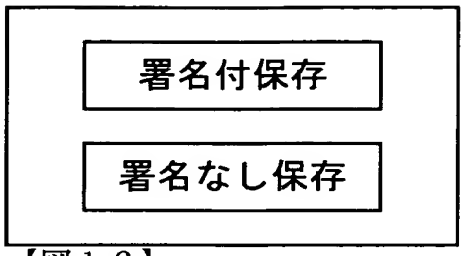
【図１３】


開始
S1301
ﾃﾞｰﾀに電子署名を行う？
NO
YES
S1302
秘密鍵を新規に作成する？
NO
YES
S1306
ｼｽﾃﾑに保存された秘密鍵を選択
S1303
秘密鍵暗証番号の入力
S1304
秘密鍵の作成・保存
S1307
公開鍵が存在する？
NO
YES
S1305
公開鍵の作成・保存
S1308
ﾒｯｾｰｼﾞﾀﾞｲｼﾞｪｽﾄ値の算出
S1309
秘密鍵にてﾒｯｾｰｼﾞﾀﾞｲｼﾞｪｽﾄ値を暗号化
S1310
暗号化ﾒｯｾｰｼﾞﾀﾞｲｼﾞｪｽﾄ値をﾒﾓﾘｶｰﾄﾞに保存
S1311
画像ﾌｧｲﾙﾃﾞｰﾀをﾒﾓﾘｶｰﾄﾞに保存
S1312
ﾌﾟﾘﾝﾄｼﾞｮﾌﾞﾃﾞｰﾀの作成?
NO
YES
S1313
ﾌﾟﾘﾝﾄｼﾞｮﾌﾞﾃﾞｰﾀ作成・保存
終了

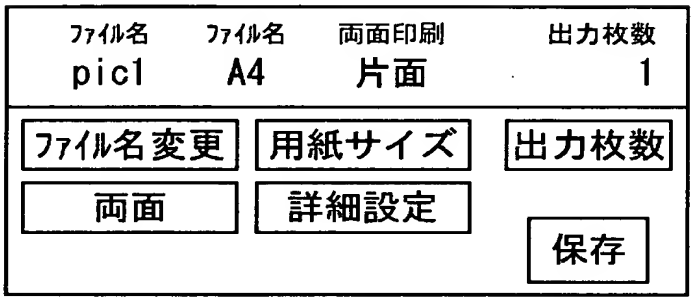
【図１４】


開始
S1401
秘密鍵・公開鍵を保存・表示？
NO
YES
S1402
ユーザに保存・表示形態について確認
S1403
秘密鍵をデータと同一メモリカードに保存？
YES
S1404
秘密鍵をメモリカードに保存
NO
S1405
秘密鍵をデータと別メモリカードに保存？
YES
S1406
秘密鍵保存フラグON
NO
S1407
秘密鍵を表示？
YES
S1408
秘密鍵を表示
NO
S1409
公開鍵をデータと同一メモリカードに保存？
YES
S1410
公開鍵をメモリカードに保存
NO
S1411
公開鍵をデータと別メモリカードに保存？
YES
S1412
公開鍵保存フラグON
NO
S1413
公開鍵を表示？
YES
S1414
公開鍵を表示
NO
S1415
秘密鍵フラグON or 公開鍵フラグON ？
YES
S1416
メモリカード交換指示
S1417
フラグONの鍵をメモリカードに保存
NO
終了

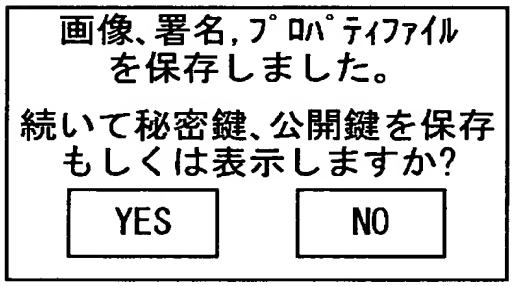
【図１５】



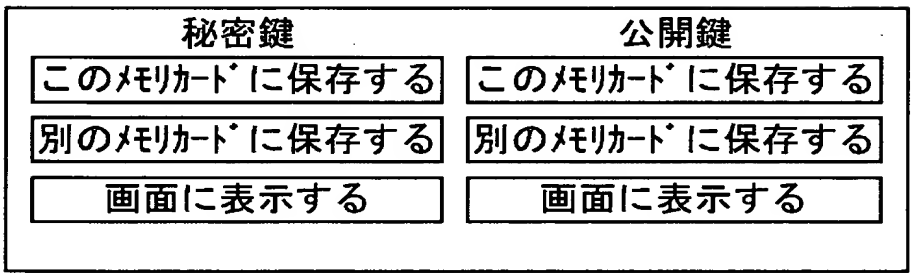
【図１６】



【図１７】



【図１８】



【書類名】　　要約書

【要約】

【課題】　メモリカード内の画像ファイルデータの改ざん・偽造を判別できるようにして、画像出力の信頼性を向上させる。

【解決手段】　メモリ媒体に蓄積されている画像ファイルデータに関する電子署名、上記電子署名に用いた秘密鍵、またはその対となる公開鍵を、上記画像ファイルデータ及びプロパティファイルとともに画像制御装置に転送する転送手段と、上記転送手段によって転送された情報に基づいて画像出力を行うように制御する画像出力制御手段とを設け、メモリ媒体に格納されている画像ファイルデータの改ざん・偽造を防止できるようにする。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００１００７〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都大田区下丸子３丁目３０番２号
氏　名　キヤノン株式会社